

AMENDED IN ASSEMBLY APRIL 3, 2008

CALIFORNIA LEGISLATURE—2007–08 REGULAR SESSION

ASSEMBLY BILL

No. 2362

Introduced by Assembly Member Keene

February 21, 2008

An act to amend Section ~~1798.14~~ 1798.29 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL’S DIGEST

AB 2362, as amended, Keene. State records: ~~personal information.~~
information: security breaches.

Existing law, the Information Practices Act of 1977, requires that any agency that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways any breach of security of the data, as defined, to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law authorizes an agency to provide that disclosure by written notice, by electronic notice, or, upon a specified condition, by substitute notice.

This bill would require an agency, when collecting personal information from a resident to provide notice to the resident that his or her personal information is being handled in a secure manner that guards against unauthorized disclosure and that in the event of a breach of the security of the system, timely and appropriate notice will be provided. By adding to the procedures local agencies must follow when collecting personal information, this bill would impose a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state.

Statutory provisions establish procedures for making that reimbursement.

This bill would provide that, if the Commission on State Mandates determines that the bill contains costs mandated by the state, reimbursement for those costs shall be made pursuant to these statutory provisions.

~~Existing law, the Information Practices Act of 1977, prohibits specified state agencies from disclosing any personal information in a manner that would link the information disclosed to the individual to whom it pertains. It requires that each agency maintain in its records only personal information which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.~~

~~This bill would make a technical, nonsubstantive change to these provisions.~~

Vote: majority. Appropriation: no. Fiscal committee: ~~no~~-yes.
State-mandated local program: ~~no~~-yes.

The people of the State of California do enact as follows:

1 *SECTION 1. Section 1798.29 of the Civil Code is amended to*
2 *read:*

3 1798.29. (a) Any agency that owns or licenses computerized
4 data that includes personal information shall disclose any breach
5 of the security of the system following discovery or notification
6 of the breach in the security of the data to any resident of ~~California~~
7 *this state* whose unencrypted personal information was, or is
8 reasonably believed to have been, acquired by an unauthorized
9 person. The disclosure shall be made in the most expedient time
10 possible and without unreasonable delay, consistent with the
11 legitimate needs of law enforcement, as provided in subdivision
12 (c), or any measures necessary to determine the scope of the breach
13 and restore the reasonable integrity of the data system.

14 (b) Any agency that maintains computerized data that includes
15 personal information that the agency does not own shall notify the
16 owner or licensee of the information of any breach of the security
17 of the data immediately following discovery, if the personal
18 information was, or is reasonably believed to have been, acquired
19 by an unauthorized person.

1 (c) The notification required by this section may be delayed if
2 a law enforcement agency determines that the notification will
3 impede a criminal investigation. The notification required by this
4 section shall be made after the law enforcement agency determines
5 that it will not compromise the investigation.

6 (d) For purposes of this section, “breach of the security of the
7 system” means unauthorized acquisition of computerized data that
8 compromises the security, confidentiality, or integrity of personal
9 information maintained by the agency. Good faith acquisition of
10 personal information by an employee or agent of the agency for
11 the purposes of the agency is not a breach of the security of the
12 system, provided that the personal information is not used or
13 subject to further unauthorized disclosure.

14 (e) For purposes of this section, “personal information” means
15 an individual’s first name or first initial and last name in
16 combination with any one or more of the following data elements,
17 when either the name or the data elements are not encrypted:

18 (1) Social security number.

19 (2) Driver’s license number or California Identification Card
20 number.

21 (3) Account number, credit or debit card number, in combination
22 with any required security code, access code, or password that
23 would permit access to an individual’s financial account.

24 (4) Medical information.

25 (5) Health insurance information.

26 (f) (1) For purposes of this section, “personal information” does
27 not include publicly available information that is lawfully made
28 available to the general public from federal, state, or local
29 government records.

30 (2) For purposes of this section, “medical information” means
31 any information regarding an individual’s medical history, mental
32 or physical condition, or medical treatment or diagnosis by a health
33 care professional.

34 (3) For purposes of this section, “health insurance information”
35 means an individual’s health insurance policy number or subscriber
36 identification number, any unique identifier used by a health insurer
37 to identify the individual, or any information in an individual’s
38 application and claims history, including any appeals records.

39 (g) For purposes of this section, “notice” may be provided by
40 one of the following methods:

1 (1) Written notice.

2 (2) Electronic notice, if the notice provided is consistent with
3 the provisions regarding electronic records and signatures set forth
4 in Section 7001 of Title 15 of the United States Code.

5 (3) Substitute notice, if the agency demonstrates that the cost
6 of providing notice would exceed two hundred fifty thousand
7 dollars (\$250,000), or that the affected class of subject persons to
8 be notified exceeds 500,000, or the agency does not have sufficient
9 contact information. Substitute notice shall consist of all of the
10 following:

11 (A) E-mail notice when the agency has an e-mail address for
12 the subject persons.

13 (B) Conspicuous posting of the notice on the agency's Web site
14 page, if the agency maintains one.

15 (C) Notification to major statewide media.

16 (h) Notwithstanding subdivision (g), an agency that maintains
17 its own notification procedures as part of an information security
18 policy for the treatment of personal information and is otherwise
19 consistent with the timing requirements of this part shall be deemed
20 to be in compliance with the notification requirements of this
21 section if it notifies subject persons in accordance with its policies
22 in the event of a breach of security of the system.

23 (i) *When collecting personal information from a resident of this*
24 *state, an agency shall provide notice to the resident that his or her*
25 *personal information is being handled in a secure manner that*
26 *guards against unauthorized disclosure and that in the event of a*
27 *breach of the security of the system, timely and appropriate notice*
28 *shall be provided.*

29 *SEC. 2. If the Commission on State Mandates determines that*
30 *this act contains costs mandated by the state, reimbursement to*
31 *local agencies and school districts for those costs shall be made*
32 *pursuant to Part 7 (commencing with Section 17500) of Division*
33 *4 of Title 2 of the Government Code.*

34 ~~SECTION 1. Section 1798.14 of the Civil Code is amended~~
35 ~~to read:~~

36 ~~1798.14. Each agency shall maintain in its records only~~
37 ~~personal information that is relevant and necessary to accomplish~~

- 1 ~~a purpose of the agency required or authorized by the California~~
- 2 ~~Constitution or statute or mandated by the federal government.~~

O